FCMB GROUP PLC

FCMB Group Plc. (“The Holding Company”)

ANTI-MONEY LAUNDERING/COUNTERING THE FINANCE OF TERRORISM (AML /CFT) FRAMEWORK

FCMB GROUP PLC

REVISION HISTORY

Initiated By	Date	Description	Initial Version	Comment	Current Version
Risk Management & Compliance	Dec 2013	AML/CFT Framework	1.0		1.0
Next Review Date: To be reviewed yearly					

FCMB GROUP PLC

Table of Contents

FCMB GROUP PLC

Introduction

Strategic Intent and Corporate Objectives

Risk management is an increasingly important business driver and business stakeholders have now become much more aware of the importance of risk. Thus, the risk management at FCMB Group Plc is very crucial and critical to the achievement of the Group's vision, mission, strategic business objectives, ensure sustainability of such, identify and explore growth opportunities and manage inherent challenges and threats in operational and business environments, ensure compliance with technology, corporate governance standards and regulatory norms and pronouncements. The framework is to strengthen the administration and supervision of AML/CFT risk management and compliance and to support the subsidiaries to ensure that the group corporate governance principles, risk culture, risk appetite and risk management processes are implemented in line with the board and regulatory's expectations.

It will also provide management with clear, comprehensive and unbiased analysis of the adequacy, existence and effectiveness of internal controls and processes to track, report and manage AML/CFT risks in line with the expectations of the regulatory authorities and board of directors. As such, this document sets out procedures for identifying, assessing, monitoring, managing and reporting AML/CFT risks within FCMB Group Plc. (FCMB).

The Group

FCMB Group Plc. (the Group) is a non-operating Holding Company incorporated in 2012 with three wholly-owned operating entities, namely First City Monument Bank Limited (Bank), FCMB Capital Markets Limited and CSL Stockbrokers Limited (CSLS). The Group is one of the leading financial services institutions in Nigeria, with following subsidiaries that are market leaders in their respective segments.

1 First City Monument Bank Limited (Direct)
2 FCMB Capital Markets Limited (Direct)
3 CSL Stockbrokers Limited (Direct)

4 FCMB UK Limited (Indirect)
5 Credit Direct Limited (Indirect)
6 First City Asset Management Limited (Indirect)
7 CSL Trustee Limited (Indirect)

The number of shareholders of the Group is almost 530,000 with a total unit of shares of over 19.8 billion with a customer base of over 2 million customers, 275 branches and cash-centres spread across every state in Nigeria and presence in the United Kingdom, through its Financial Conduct Authority (FCA)-authorised banking subsidiary (FCMB UK Ltd). As at 31 December 2013, the amount of shareholders' funds is N143.7 billion. The Group and its operating entities have as regulators the Central Bank of Nigeria (CBN), Securities and Exchange Commission (SEC) and Nigerian Stock Exchange (NSE)

Vision

The Group's vision is:

"To be the premier financial services group of African origin"

The Group aspires to be a world-class and first-rate financial institution achieving superior financial performance and returns for the shareholders and other stakeholders. The Group seeks to be in the top 5 financial institutions in Africa by 2030 by market capitalization and offering best customer experience in Nigeria

Mission

"To attain the highest levels of customer advocacy, be a great place to work, and deliver superior and sustainable returns to our shareholders"

The Group shall transfer customer experience into loyalty through provision of superior and delightful service delivery to build a mutually beneficial and enduring long term relationship.

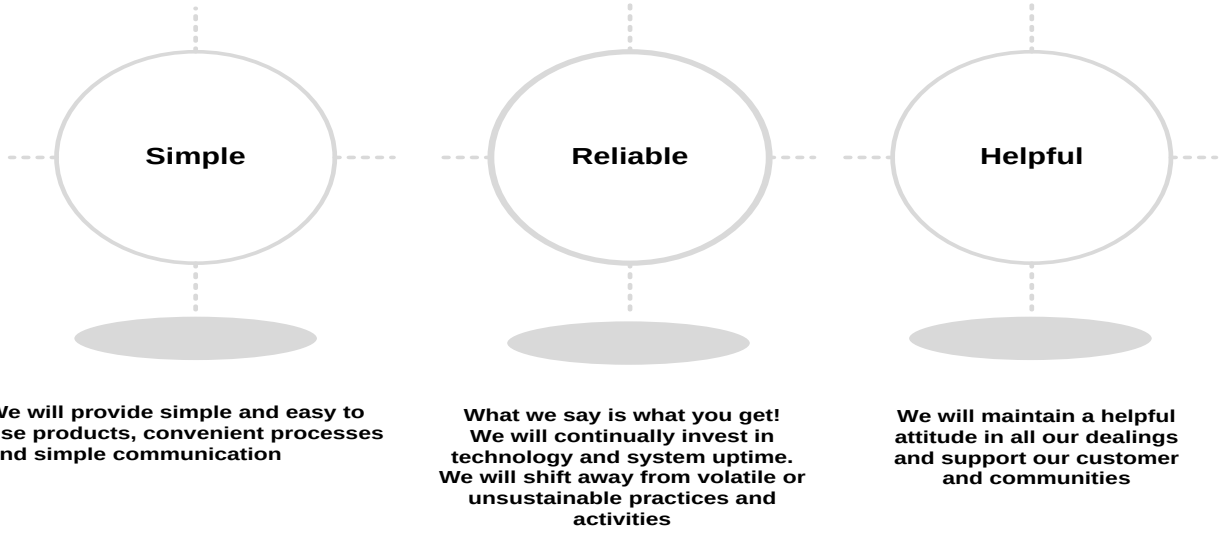
Strategic Priorities

For the planning period 2014 – 2016, the Group has defined 9 main strategic priorities:

- ✓ Continually improve customer experience
- ✓ Accelerate growth in products and services
- ✓ Improve management of operational cost
- ✓ Reduce the cost of risk
- ✓ Possess the most valuable retail franchise in the country
- ✓ Transform and build a winning culture
- ✓ Materially grow annuity sources of income in investment bank
- ✓ Increase distribution capacity and productivity
- ✓ Intensify growth in assets

Our Customer Promise

We want all our customers to see and experience us as being:



Corporate Core values

The Group's corporate values are derived from the Group's corporate vision, mission and the goals and business objectives. The core values that provide the guidance for business activity and culture in the Group are summarised as follows:

Professionalism	• Play by **the rules**
Sustainability	• Develop **capacity to endure** through **innovation and creativity** • Create and maintain **an environment that promotes ingenuity.**
Customer Focus	• Customer sets **our priorities**
Excellence	• Aim for **the highest standards** in our business and operational activities and processes

Figure 1: Enterprise Risk Management Structure

About AML/CFT Manual

This AML/CFT Manual ("the Manual" or "this Manual") sets out a high-level framework for the disciplined, continuous and consistent management of regulatory and compliance risk at FCMB Group Plc. ("The Group"). It has been defined and written in line with the commitment of the Board of Directors ("the Board") and the Management of the Group to establish and put in place sustainable best practices in Risk Management that is at par with foremost international institutions in our industry. In preparing this manual, appropriate attention has been given to recent changes in the regulatory environment-both local and international-including theBasel Committee on Banking Regulations and Supervisory Practices, the Wolfsberg Group principles, Financial Action Task Force recommendations, provisions of the Money Laundering (Prohibition) Act as amended and CBN AML/CFT Regulations and the requirements for better risk management practices as issued by the local regulators.

This manual forms an integral part of the group's Enterprise-wide Risk Management Framework.

The essence of this AML/CFT Manual is to:

a. Document the comprehensive and constantly evolving policies, procedures and processes deployed by the Group to assure adherence to the provisions of AML/CFT legislations and guidelines in Nigeria and all jurisdictions where our businesses are located.

b. Create a framework for managing AML/CFT compliance risks in the Group.

c. Ensure that the Group does not fall victim of illegal activities perpetrated by its customers.

The manual provides members and staff of the Group with adequate and comprehensive guidance on AML/CFT compliance risks to ensure that the actions of the Group with respect to compliance risk management are consistent with the Group's strategy business objectives, risk appetite statement, and regulatory requirements. The issues covered in the framework are integral to the processes of identification, measurement, controlling and monitoring of its risks.

The key elements of the Group's AML/CFT Framework addressed in the manual include:

- Money Laundering
- Terrorism and Terrorism Financing
- Regulatory and Legal Framework
- Customer Identification Program
- Reporting Suspicious Transactions
- Awareness and Training
- Correspondent Banking Relationship
- Politically Exposed Persons
- Designated Non-Financial Businesses and Persons.

In developing this framework, significant emphasis was placed on:

- establishing a strong, independent compliance function to champion, coordinate and monitor the enterprise-wide AML/CFT risk across the Group and subsidiaries;
- formally assigning accountability and responsibility for AML/CFT risk management; and

Ownership of the Manual

Ownership of this manual rests with the Group's Head – Risk Management and Compliance Department (HRMCD). He shall be responsible for the implementation of the AML/CFT framework across the Group under the direct supervision of the Group Managing Director.

Updating the AML/CFT Manual

The evolving nature of AML/CFT risks and the dynamic characteristics of the operating environment necessitate regular review of the effectiveness of the AML/CFT process. Risk responses and controls that were once effective may become inadequate or irrelevant and as such control activities may become less effective, and the Group's strategy and objectives may also have changed. In the light of this, the Group's AML/CFT Framework manual shall be subject to continuous review, especially in line with expectation of the relevant regulatory authorities to ensure effective and innovative risk management practices.

The reassessment shall be done using either or a combination of the two approaches listed below:

- Continuous self-assessment, evaluation and monitoring by the Risk Management and Compliance and Internal Audit Departments and;
- Independent evaluation by third parties.

Under the continuous self-evaluation, ongoing monitoring of this manual shall be part of the normal, recurring strategic activities of the Group. On the other hand, the frequency of independent evaluations required for management to have reasonable assurance about the effectiveness of the Group's AML/CFT compliance shall be a matter of management's judgment.

In making that determination, management shall consider the nature and degree of changes occurring, from both internal and external events, and their associated risks.

The purposes of the review and update shall be to determine the following:

- The appropriateness and sufficiency of the AML/CFT framework;
- The appropriateness of the Group's risk assessment engine given the nature, scope and complexity of the Group's activities;
- The accuracy or integrity of data being used; and
- The reasonableness of scenarios and assumptions.

Roles and Responsibilities for the AML/CFT review

The Group's Head – Risk Management & Compliance Department (HRMCD) has the primary responsibility for risk management and shall assume responsibility for the review and amendment of the AML/CFT framework. In addition, the Head - Internal Audit Department may propose changes to the framework based on the outcome of his review. However, these proposed changes must receive the approval of the HRMCD, the Executive Management Committee and the Board Risk, Audit & Finance Committee.

The executive management committee shall endorse any proposed amendment before the board approval. The Board, through the Board Risk, Audit & Finance Committee shall approve all amendments to the Group's AML/CFT Framework.

Important Regulatory and Mandatory References

i. Central Bank of Nigeria (CBN)
ii. Nigeria Stock Exchange (NSE)
iii. Securities and Exchange Commission (SEC)
iv. Financial Action Task Force (FATF)
v. International Financial Reporting Standards (IFRS) /International Accounting Standards (IAS)
vi. CBN Prudential Guidelines
vii. Basel Accord (Basel I, Basel II, Basel III & Basel IV)
viii. Enterprise risk management frameworks and relevant policies and procedures of the subsidiaries
ix. And any other relevant laws and guidelines as issued by relevant authority

Definition of Terms and Acronyms

i. **Anti-Money Laundering (AML):** Refers to policies, procedures and controls which are instituted to prevent, detect and report money laundering activities.

ii. **Central Bank of Nigeria (CBN):** The apex bank of Nigeria and a regulator to all banks in Nigeria. It supervises all Banking practices and operations as it relates to Banks and the public or bank and another Bank or between a Bank and itself.

iii. **Chief Compliance Officer (CCO):** A senior official who is a Statutory Officer by virtue of Section 9(1a) of MLPA 2011, who interfaces between Management and Staff, Organizations, Regulatory and Law Enforcement Agencies on all issues pertaining to money laundering and financing of terrorism.

iv. **Compliance Officer (CO):** A statutory official of a financial institution by virtue of Section 9(1a) of MLPA 2011, who interfaces with staff and Organizations, Regulators and Law Enforcement Agencies on all issues pertaining to money laundering and reports to the CCO.

v. **Customer Due Diligence (CDD):** This means taking steps to identify your customer and checking that they are who they say they are. In practice this means obtaining the following from a customer:
   - Name
   - Photograph on an official document which confirms his identity
   - Residential address

vi. **Currency Transaction Reports (CTRs):** This is made by financial institutions and designated non-financial institutions regarding any transaction, lodgment or transfer of funds in excess of N5,000,000 or its equivalent, in the case of an individual, or N10,000,000 in the case of a corporate body pursuant to Section 10 of the ML(P)A, 2011.

vii. **Economic and Financial Crimes Commission (EFCC):** A Federal Government agency which is charged with the responsibility of coordinating the various Institutions involved in the fight against money laundering and enforcement of all laws dealing with economic and financial crimes.

viii. **Financial Action Task Force (FATF):** FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. It was established in 1989 by the G-7 Summit that was held in Paris. As a “policy making body” it works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. It

is kn\own for its 46 recommendations which establish an AML framework for its member countries. (See Appendix 1 for FATF 40 Recommendations)

ix. **Know Your Customer (KYC):** Entails obtaining and verifying customer identity, Preservation of records of customers, mandatory disclosure of transactions to authorized statutory bodies.

x. **Know Your Customer's Business (KYCB):** Another offshoot from the KYC where financial institutions are enjoined to know the line of business of their customers such that transactions by the customers are fairly predictable. This will assist in the identification of unusual transactions or activities that may appear inconsistent with the customer's known business.

xi. **Money Laundering (Prohibition) Act (MLPA) 2011:** A Federal legislation which deals on the policies, framework and sanctions on Money laundering for both Financial Institutions and Designated Non-Financial Persons and Businesses (DNFPBs)

xii. **National Drug Law Enforcement Agency (NDLEA):** A Federal Government agency which is charged with the responsibility of coordinating the various Institutions involved in the fight against illicit drugs and enforcement of all laws dealing with such crimes.

xiii. **Nigeria Financial Intelligence Unit (NFIU):** The Nigerian arm of the global Financial Intelligence Unit (FIU). It is domiciled within the Economic and Financial Crimes Commission (EFCC) as an autonomous unit. The activities of the NFIU are covered under the EFCC Act 2004 and MLPA 2011. Its core role is that it serves as the country's central agency for the intelligence information gathering, collection, analysis and dissemination of financial information regarding money laundering and the financing of terrorism.

xiv. **Politically Exposed Persons (PEPs):** This involves individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of Government, Politicians, Senior Government Official, Judicial or Military Officials, Senior Executives of State Owned Corporations, important Political Party Officials and any "close associate" of a senior political figure (local/foreign) all fall into this category.

xv. **Suspicious Transaction Reports (STRs):** This is made by financial institutions and designated non-financial institutions or made voluntarily by any person irrespective of the amount involved pursuant to Section 6 of the MLPA, 2011. It is a transaction, which

is inconsistent with a customer's known legitimate business or personal activities. The first key to the recognition of a suspicious transaction is in knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

xvi. **Shell Company** – Any financial institution or bank with no fixed (physical) and registered address.

FCMB GROUP PLC

1 *Introduction*

Regulatory/Compliance Risk is the risk that the Group may suffer loss as a result of its failure to comply with the letter and spirit of laws, regulations, rules, and codes of conduct applying to its business activities

The risk of non-compliance with relevant laws and regulatory guidelines can result in potential financial losses arising from reputational damage, regulatory fines and sanctions, customer run, loss of business and/or franchise, litigation and as such, FCMB group remains committed to fully compliance with all relevant laws, regulatory pronouncements and requirements especially as they concern AML/CFT and KYC and its internal policies on such and to always act with care and due diligence.

2 *Group Policy Statement*

a. Implementing sound anti-money laundering and countering financing of terrorism & proliferation policies and procedures which will ensure that it is not used as a conduit for money laundering or financing of other illicit businesses;

b. Implementing policies, procedures, guidelines and provisions of manuals emanating from relevant regulatory bodies towards ensuring compliance with all domestic and international laws and regulations on money laundering and countering financing of terrorism and proliferation in order to mitigate AML/CFT risks it is exposed to;

c. Full compliance with both the letter and the spirit of all regulatory requirements and high standard of market conduct;

d. Conducting all the Group businesses in accordance with all regulatory policies and guidelines governing its operating environment;

e. Giving full cooperation to law enforcement authorities within the limits of the rules governing confidentiality;

f. Effective communication of these policies towards raising the level of staff awareness on AML/CFT issues;

g. Retention and preservation of records of customers' transactions for a minimum of five years or as may be prescribed by various regulatory bodies;

h. Exiting relationships which pose heightened money laundering risks to the group and reporting same to the relevant regulatory agencies.

Drawing significantly from recommendations of the Basel Committee on Banking Regulations and Supervisory Practices, the Wolfsberg Group principles, Financial Action Task Force recommendations, provisions of the Money Laundering (Prohibition) Act as amended and CBN AML/CFT Regulations, the Group has put in place the following measures in the attainment of its objective of ensuring full compliance with the letter and the spirit of all applicable laws and regulations.

- **The Group**

(i) Has established sound internal policies, controls, procedures to mitigate money laundering and financing of terrorism risks.
(ii) Regularly trains its staff to identify suspicious activities/transactions and to take appropriate actions.
(iii) Has in place and updates the AML/CFT Employee Training Programmes for new hires and regular refresher training for existing staff.
(iv) Has internal referral process and procedures for compliance matters.
(v) Ensures implementation of policies and procedures and internal controls to correct/enhance and/or adapt to regulatory changes / deficiencies.
(vi) Has designated a senior management staff as its Chief Compliance Officer to oversee its AML/CFT program

3 *Compliance Role and Responsibilities*

- **The Board**

The roles and responsibilities of the Board of Directors with respect to AML/CFT Compliance Risk Management include (but shall not be limited to):

(i) Assume overall accountability for Compliance performance
(ii) Ensure that appropriate AML/CFT Compliance Risk Management framework is established and is in operation
(iii) Approve the AML/CFT Compliance Risk Management program and policies
(iv) Provide guidelines regarding the management of AML/CFT Compliance risks
(v) Appoint and designate a Chief Compliance Officer to coordinate and monitor AML/CFT Compliance at subsidiary level

- **Chief Compliance Officer**

(i) Coordinate and monitor AML/CFT Compliance
(ii) Inform Board and Management of AML/CFT Compliance efforts, compliance failures and the status of corrective actions
(iii) Monitor implementation of the code of corporate governance
(iv) Ensure implementation of Board decisions on compliance matters
(v) Ensure that regulatory changes are effectively implemented
(vi) Direct prompt investigation of any unusual or suspicious transaction and reports to the Regulatory body
(vii) Ensure that compliance requirements are integrated into the day to day activities of the institution and that processes are efficient and in accordance with applicable laws and policies.

- **AML/CFT Compliance Officer**

(i) Coordinate and monitor day to day compliance with applicable money laundering laws and regulations
(ii) Monitor transactions to detect any unusual or suspicious transactions.
(iii) Conduct Preliminary investigation on any unusual or suspicious transaction.

(iv) Prompt preparation and delivery of all relevant returns to the regulatory bodies in line with the MPLA 2011 and CBN AML/CFT Regulation (2009) as amended.

(v) Communicate AML/CFT issues to all stakeholders

- **Branch Compliance Officers**

All Customer Service Managers are designated as compliance officers in their respective branches and shall perform the following functions:

(i) Monitor money laundering activities in the branch

(ii) Ensure adherence to KYC and KYCB principles.

(iii) Coordinate submission of suspicious transactions report to the Chief Compliance Officer.

(iv) Coordinate collation of documents as may be requested from time to time.

(v) Ensure full implementation of the Group's policy and statutory regulations on compliance and money laundering activities.

(vi) Ensure swift resolution of corrective action grid on all inspection reports i.e. statutory/Group reports, e.g. CBN, NFIU, NDIC, Group Internal Audit Reports, Control reports, etc.

(vii) Create awareness among branch staff on Compliance and anti-money laundering activities.

- **Group Internal Audit**

(i) Incorporate compliance testing in their normal audit program.

(ii) Report on results of the independent testing to the Board through the GMD/CEO

- **All Employees:**

(i) Be aware of and comply with the Group's policies and procedures.

(ii) Report suspected money laundering activities to the Chief Compliance Officer

(iii) Comply strictly with Know-Your-Customer directives.

4 *Anti-Money Laundering and Countering Financing of Terrorism Policies*

4.1 Money Laundering

Money Laundering is the process by which monies or assets derived from criminal activities are converted into funds or assets which appear to have a legitimate origin. It involves taking criminal proceeds and disguising their illegal sources in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities.

4.2 Money Laundering Predicate Offence

Money laundering predicate offence is the underlying criminal activity that generates proceeds, which when laundered, results in the offence of money laundering. These include kidnapping, illegal restraint and hostage taking, insider trading and market manipulation, embezzlement & fraud, bribery and corruption, robbery, drug trafficking, environmental crimes, terrorism, counterfeiting currency, counterfeiting and piracy of products, smuggling, extortion, forgery, sexual exploitation, etc.

4.3 Stages of Money Laundering

a) **Placement:** The physical disposal of cash/property derived from criminal activity. The purpose of this stage is to introduce proceeds into the traditional or non –traditional financial system without attracting attention e.g. purchase of artwork, cash deposits, casinos etc.
b) **Layering:** This involves separating source of proceeds from ownership by changing the form. This is designed to hamper audit trail e.g. complex wire transfers, resell of assets/properties, opening of several accounts to disguise origin of funds etc.
c) **Integration:** Re – channeling the laundered funds back to the financial system as legitimate funds.

4.4 Terrorism and Terrorism Financing

a) **Terrorist Act:** Any act intended to cause death or serious bodily injury to a civilian or any other person not taking an active part in the hostilities. Usually, the purpose is to intimidate a population or to compel a government or society to do or abstain from doing any act
b) **Terrorism financing (TF):** occurs when a person by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such the funds will be used or in the knowledge that the funds will be used in full or in part, in order to carry out a terrorist act.
c) Terrorist activities are sometimes funded from the proceeds of illegal activities. Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.
d) Difference between Money Laundering and Terrorism Financing illustrated in Figure 9 below:

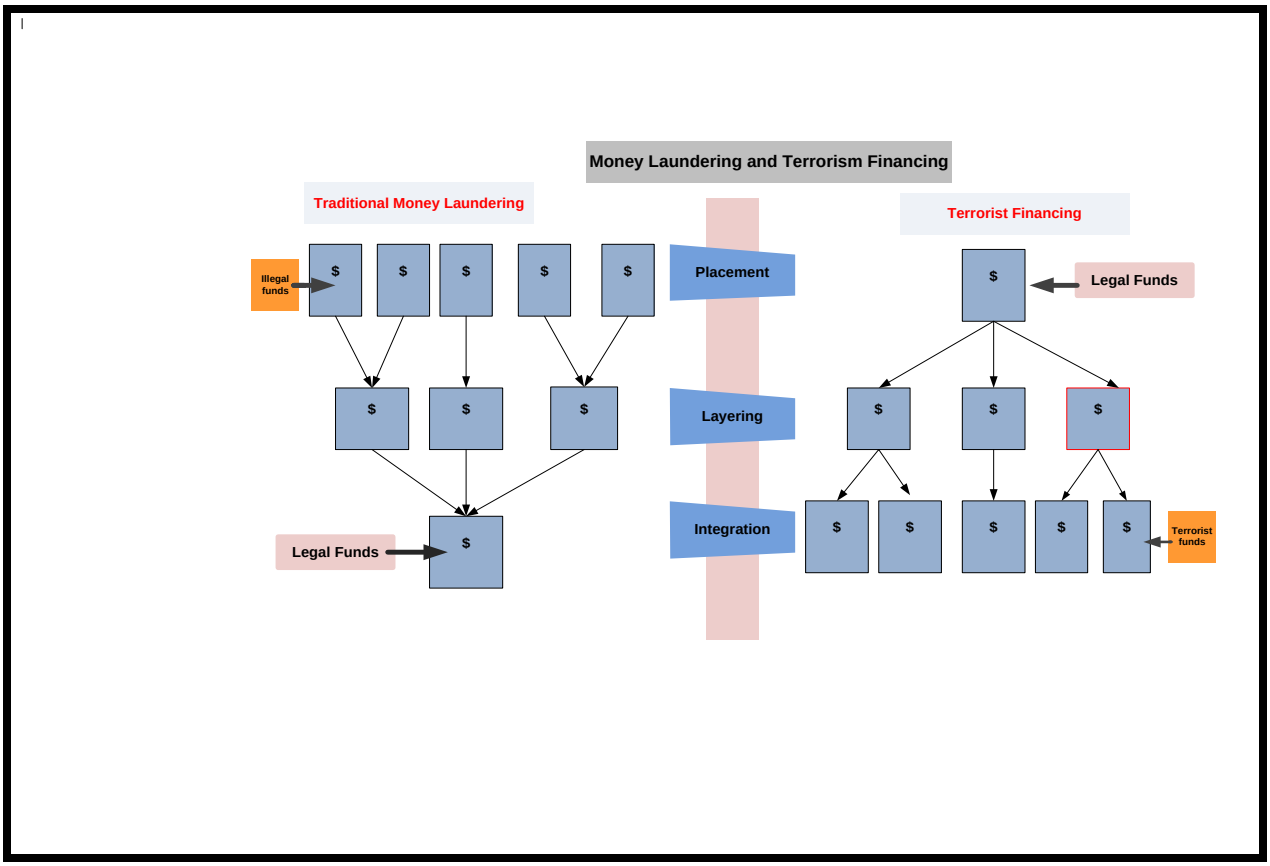


Figure 2: Money Laundering and Terrorism Financing

5 *Regulatory and Legal Frameworks*

Nigerian financial institutions are monitored for money laundering by some organizations/agencies and under the provisions of the regulations specified below:

5.1 Institutional Framework - Local

1) Economic and Financial Crimes Commission (EFCC)
2) Nigeria Financial Intelligence Unit (NFIU)
3) National Drug Law Enforcement Agency (NDLEA)
4) Central Bank of Nigeria (CBN)
5) Federal Ministry of Commerce (FMC)
6) Independent Corrupt Practices Commission (ICPC)

7) Federal Inland Revenue Services (FIRS)
8) National Insurance Commission (NAICOM)
9) Nigeria Customs Service (NCS)
10) Nigeria Immigration Services (NIS)
11) Nigeria Deposit Insurance Corporation (NDIC)
12) Securities and Exchange Commission (SEC)

5.2 Institutional Framework – International

1) Basel Committee on Banking Supervision
2) Financial Action Task Force (FATF)
3) Inter-Governmental Group Against Money Laundering (GIABA)
4) Egmont Group (of Financial Intelligence Units)
5) Wolfsberg Group
6) United Nations Office of Drugs and Crime (UNODC)
7) The World Bank
8) European Union
9) Interpol
10) The Joint Money Laundering Steering Group

5.3 Legal Framework – Local

1) Money Laundering (Prohibition) Act 2011
2) Terrorism (Prevention) Act 2011
3) CBN AML/CFT Regulation 2009
4) SEC Rules and Regulations 2013
5) NSE Rules and Regulations
6) Advanced Fee Fraud Act 2006
7) Bank's (recovery of Debt) and Financial Malpractices in Banks in Nigeria Act (as amended)
8) Banks and other Financial Institutions Act 1991
9) ICPC (Establishment) Act
10) EFCC (Establishment) Act 2004
11) NDLEA Act

12) Dishonored Cheques Act, etc.

5.4 Legal Framework – International

1) Directive 2005/60/EC of the European Parliament and of the Council.
2) Office of Foreign Asset Control (OFAC)
3) USA PATRIOT Act : Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
4) Sarbanes-Oxley Act
5) FATF 40 Recommendation

6 *Customer Identification Program (CIP)*

The Customer Identification Program is intended to enable the Group form a reasonable belief that it knows the true identity of each customer.

As a general rule, a business relationship with FCMB will NOT be established until the identity of a potential customer is satisfactorily established. Where a potential customer declines to provide any account initiation information, the relationship will not be established. Furthermore, if follow-up information is not forthcoming, any relationship already established will be terminated.

The Group's account opening procedures which also specify the identification documents and information required from each customer are contained in the Group's Operations Policy Manual

6.1 Know Your Customer (KYC)

KYC is the due diligence that financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information before doing financial business with them.

To this end, the Group's KYC policies and procedures emphasize the following:

i. Obtaining the necessary documents and information from every customer as specified in the Group's Operations Policy manual

ii. Prohibition of opening numbered or anonymous accounts

iii. Minimum acceptable identification evidence for low risk and low value accounts

iv. Independent verification of the legal status of incorporated entities and sole proprietorships with the Corporate Affairs Commission in writing

ii. Screening of customer information against database of individuals and entities subject to sanction (watch-list check) at on-boarding stage and quarterly customer database scan as required by the AML/CFT regulations

iii. Identifying the customer as well as the beneficial owners and verifying that customer's identity using reliable, independent source documents, data or information

iv. Profiling of customers such that transactions by our customers are fairly predictable.

v. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

vi. Customer information update whenever the need arises

vii. Obligation to report to the regulatory authorities suspicious transactions, which may ultimately have a bearing with money laundering activities

The group as a matter of policy does not transact business with "shell corporations" as described under the International Conventions.

The group applies each of the CDD measures under but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures to be taken shall be consistent with any guidelines issued by competent authorities. For higher risk categories, the group shall perform enhanced due diligence.

6.2 Record Keeping and Retention requirements

The group shall comply with the requirements of the Money Laundering (Prohibition) Act, CBN AML/CFT Regulations, SEC AML/CFT Compliance Manual for Capital Market Operators 2013

and any other legislation to the effect that all records of customers' identification and transactions must be kept for a minimum of five years after the closure of the account /severance of relationship with the customer or after carrying out transactions.

Records of all suspicious transactions shall be kept for the same period.

Requests for AML records by Regulatory and Law Enforcement Agencies

Upon request by a regulatory or law enforcement agency, the Group shall make available records related to its AML Compliance or its customers as soon as possible from the date of the request.

7 *Reporting Suspicious Transactions*

7.1 Identification of Suspicious Transactions

The group shall exercise due diligence in identifying and reporting of suspicious transaction.

Suspicious transactions shall include:

1) Transaction involving a frequency which is unjustifiable or unreasonable, unusual or has unjustified complexity.
2) Transaction which appears to have no economic justification or lawful objectives.
3) Transactions which are structured to avoid reporting and record keeping requirements.
4) Transfers of foreign currency transactions which are recalled twice from the account of a customer by correspondent bank. (Note that a first recall could be due to error.)
5) If the circumstances surrounding the first recall of a foreign currency transactions from the account of a customer by correspondence bank appeared suspicious.
6) Altered or false identification or inconsistent information or any transaction involving criminal activity in the view of the group

7.2 Procedures for Disclosure of Suspicious Transactions

1) Any Officer of the group who suspects any transaction to be suspicious shall make an immediate report to his/her Chief Compliance Officer. If it occurred at the branches, it shall be drawn to the attention of the Compliance Officer of the branch and then to the Chief Compliance Officer through the Money Laundering Reporting Officer in Head Office.
2) The group has also established procedures whereby such reports are coordinated through a central point Money Laundering Reporting Officer domiciled in the Head Office for onward reporting to the NFIU/EFCC.
3) In the event that urgent disclosure is required in a 'live' situation, particularly when the account concerned is part of an on-going investigation, an initial notification shall be made by telephone to the Commission.
4) Staff must not disclose to customers or anyone else that they are subject to money laundering investigation. (Tipping off)
5) The group has also deployed an Anti-Money Laundering solution (SAS Money Laundering Detection application) which is a rules based application to monitor customers' transactions and flags potential suspicious transactions for monitoring by analysts. Alerts generated are reviewed and decisions to file STRs or not are documented.

7.3 Compilation of Reports and Returns to Regulatory Authorities

The group shall ensure timely and accurate rendition of all AML/CFT returns as specified in the CBN AML/CFT Regulations 2009 (as amended), the Money Laundering (Prohibition) Act 2011, the SEC Rules and Regulations as well as other relevant Regulations/Acts/Guidelines/Circulars that may be issued from time to time by various government agencies. (See the Group's Regulatory Returns Universe)

8 *Awareness and Training*

The Money Laundering (Prohibition) Act 2011 requires financial institutions to ensure, first, that its employees are made aware of the provisions of the relevant legislation and the obligations imposed on staff and financial institutions. Secondly, staff shall be given training on how to recognize and deal with transactions which may be related to money laundering or terrorist financing.

The Group's AML/CFT training program is a mix of e-learning and instructor-led training modules. The trainings incorporate current developments and changes to the MLPA 2011 and CBN AML/CFT Regulations 2009 and other related guideline. Changes to internal policies, procedures, processes and monitoring systems are also covered during the trainings

All staffs are required to complete the AML/CFT training at least once in every financial year as this forms an integral part of the Group's employee appraisal system. Evidence of completion and records of attendance shall be kept by the Training Academy and shall be made available to Compliance unit on request.

The group shall also utilize other avenues such as e-mails, compliance newsletters to disseminate compliance issues arising from new rules and regulations to all staff.

9 *Correspondent Banking Relationship*

The Group shall ensure that Correspondent-banking relationships are carefully selected. The Group prohibits dealing with shell companies*.

*Shell company is a bank or financial institution that has no physical presence in any country or is not regulated.

10 *Politically Exposed Persons (PEP)*

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of government, senior

politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and any “close associate” of a senior political figure (local/foreign). Business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves.

1) **A senior political figure:** This includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior political figure (local/foreign).
2) **Immediate Family:** The “immediate family” of a senior political figure typically includes the figure’s parents, siblings, spouse, children, and in-laws.
3) **Close Associate:** A “close associate” of a senior political figure is a person who is widely publicly known to maintain an unusually close relationship with the senior political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior political figure. Although close associates are more difficult for the Group to identify, they include individuals who, due to the nature of their relationship with the PEP, are in a position to conduct significant domestic and international financial transactions on behalf of the PEP.

The term PEP includes persons whose current or former position can attract publicity beyond the borders of a country and whose financial circumstances may be the subject of additional public interest.

Examples of PEPS includes, but not limited to the following:

1) Heads of State or Government and Cabinet Ministers
2) Governors
3) Local Government Chairmen
4) Senior Politicians
5) Senior Government Officials
6) Judicial or Military Officials
7) Senior Executives of State owned Corporations
8) Important Political Party officials
9) Family members or close associates of PEPS
10) Members of Royal Families.

10.1 Risk in doing business with PEP

Accepting and managing funds from corrupt PEPs can severely damage the Group's own reputation and can undermine public confidence in the ethical standards of the Group, since such cases usually receive extensive media attention and strong political reaction. In addition, the Group may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the Group and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

As with most aspects of compliance, the place to begin is with a risk assessment. The group conducts a risk assessment of its products/services, customers, and geographies where business is conducted. The outcome of this assessment forms the basis of a PEP/KYC compliance program.

10.2 PEP Risk Assessment

The Group assesses the risks posed to its business activities on the basis of the scope of operations and the complexity of the customer relationships. Management establishes a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities.

The following factors are considered when identifying risk characteristics of Politically Exposed Persons:

1) **Nature of the customer and the customer's business:** The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor is considered for private banking accounts opened for PEPs.
2) **Purpose and activity:** The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account.

3) **Relationship:** The nature and duration of the Group's relationship (including relationships with affiliates) with the private banking customer.
4) **Customer's corporate structure:** Type of corporate structure.
5) **Location and jurisdiction:** The location of the private banking customer's domicile and business (domestic or foreign). The review considers the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or, conversely, is considered to have robust AML standards.
6) **Public information:** Information known or reasonably available to the Group about the private banking customer. The scope and depth of this review depends on the nature of this relationship and the risks involved

10.3 Risk Minimization

1) Conducting detailed due diligence at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a "politically exposed person". The Group assesses the countries with which it has financial relationships.
2) Where the Group has business in countries vulnerable to corruption, it would establish who the senior political figures in that country are and seek to determine whether or not their customer has any connections with such individuals (for example if they are immediate family or close associates).
3) The institution is more vigilant where its customers are involved in those businesses which appear to be most vulnerable to corruption.
4) Every effort is made to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.
5) The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile would be regularly reviewed and updated.
6) A review at senior management or board level of the decision to commence the business relationship and regular review, on at least an annual basis of the development of the relationship.

7) Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.
8) Full documentation of the information collected in line with the above. If the risks are understood and properly addressed then the acceptance of such persons becomes a commercial decision as with all other types of customers.

10.4 The Group's obligations and position on PEP accounts

1) Before any account is opened for any PEP, Senior Management approval must be obtained. For this purpose, Senior Management approval must be obtained from the line Executive Director and the Chief Compliance Officer. This will be done as part of account opening formalities. No account would be opened for any PEP without the approval being in place.
2) The customers due diligence efforts do not end at account opening; ongoing account monitoring is expected. Activities on PEP accounts will be reviewed on a monthly basis with a view to identifying unusual and potentially suspicious transactions related to them and filing, as appropriate, STRs related to them.
3) Monthly returns will be sent to the CBN and NFIU on PEP transactions. This is to assist the regulators in monitoring the activities of PEPS.
4) The Group will take reasonable steps to ascertain the source of wealth and the source of funds of PEPS and report all anomalies to the CBN and other relevant authorities.
5) Periodic Enhanced Due Diligence and monitoring must be carried out on all PEPS by the RM and or AO concerned. On an annual basis, the relationship managers shall certify that none of the accounts reporting to them became PEP in the course of the year. In the event that any transaction is noted to be abnormal, such must be immediately flagged and reported to the Compliance unit immediately.
6) While circumstances will vary, certain transactions by PEPs are considered potentially suspicious and may be indicative of illegal activity.

The following guidance provides a non-exhaustive list of red flags that includes, among other things:

a) Requests to establish relationships with or route transactions through an institution that is unaccustomed to doing business with foreign persons and that has not sought out business of that type.
b) A request to associate any form of secrecy with a transaction, such as booking the transaction in the name of another person or business entity.
c) The routing of a transaction through several jurisdictions without any apparent purpose other than to disguise the nature, source, or ownership of funds.
d) The rapid increase or decrease in the funds or asset value in an account that is not attributable to market conditions.
e) Frequent or excessive use of funds transfers or wire transfers either into or out of an account.
f) Large currency or bearer instrument transactions in or out of an account.
g) The frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account.

Any situation falling into one of the above descriptions shall not automatically be treated as problematic until further investigation is done. If the facts point to a suspicious transaction, then procedures for filing a Suspicious Activity Report shall be followed and Senior Management notified of the situation.

11 *Designated Non-Financial Businesses and Professions (DNFBPs)*

1) Financial institutions are required, prior to establishing business relationship with designated non-financial businesses and Professions, to obtain evidence of registration (e.g. certificate of registration showing registration number) with the Special Control Unit on Money Laundering (SCUML) of Federal Ministry of Trade and Investments.
2) DNFBPs refer to dealers in jewelries, precious metals and precious stones, cars and luxury goods, audit firms, tax consultants, clearing and settlement companies, lawyers, notaries, other independent legal practitioners and chartered accountants, trusts and company service providers, hotels, casinos, supermarkets, real estate agents, non-governmental organizations (NGOs), religious and charitable organizations, etc.

3) The above DNFBPs customers include sole practitioners, partners and employed professionals within professional firms. They do not refer to “internal” professionals that are employees of other types of businesses or to professionals working for government agencies who may already be subject to AML/CFT measures.

12 *Audit of AML/CFT*

The Group Internal Audit (GIA) shall be responsible for review of the Group processes and transactions to ensure that they comply with CBN, NFIU/EFCC requirements on Anti-Money Laundering and Countering Financing of Terrorism.

13 *Money Laundering & Terrorist Financing Red Flags*

13.1 Potential Transactions Perceived or Identified as Suspicious

a) Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.
b) Transactions involving shell companies.
c) Transactions with correspondents that have been identified as higher risk.
d) Large transaction activity involving monetary instruments such as traveler’s cheques, bank drafts, money order, particularly those that are serially numbered.
e) Transaction with correspondents that have been identified as higher risk.
f) Transaction activity involving amounts that are just below the stipulated reporting threshold or enquires that appear to test an institution’s own internal monitoring threshold or controls.

13.2 Money laundering using cash transactions

a) Significant increases in cash deposits of an individual or corporate entity without apparent cause. Particularly if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer.

b) Unusually large deposits made by individual or a corporate entity whose normal business is transacted by cheques and other non-cash instruments.
c) Frequent exchange of cash into other currencies.
d) Customers who deposits cash through many deposits slips such that the amount of each deposit is relatively small, that overall total is quite significant.
e) Customer whose deposits contain forged currency notes or instruments
f) Customer whose deposit cash to cover applications for bank drafts.
g) Customer who regularly deposit cash to cover applications for bank drafts
h) Customers making large and frequent cash deposits but with cheques always drawn in favour of persons not unusually associated with their type of business.
i) Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.
j) Branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors.
k) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

13.3 Money laundering using deposit accounts

a) The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business;
b) Minimal, vague or fictitious information provided by a customer that the deposit money bank is not in position to verify.
c) Lack of reference or identification in support of an account opening application by a person who is unable or unwilling to provide the required documentation.
d) A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening a bank account.
e) Customer maintaining multiple accounts at a bank or different banks for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.
f) Customers depositing or withdrawing large amounts of cash with no apparent business source or in a manner inconsistent with the nature and volume of the business.

g) Accounts with large volumes of activity but low balances or frequently overdrawn positions.
h) Customers making large deposits and maintaining large balances with no apparent rationale.
i) Customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances, typically, these transactions are not consistent with the customer's legitimate business needs.
j) Sudden and unexpected increase in account activity or balance arising from deposit of cash non-cash items. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly.
k) Accounts that are used as temporary repositories for funds that are subsequently transferred outside the bank to foreign accounts. Such accounts often have low activity.
l) Customer requests for early redemption of certificate of deposit or other investment soon after the purchase, with the customer being willing to suffer loss of interest or incur penalties for premature realization of investment.
m) Customer requests for disbursement of the proceeds of certificates of deposits or other investments by multiple cheques each below the stipulated reporting threshold.
n) Retails business which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs.
o) Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks.
p) Substantial cash deposits by professional customers into client, trust or escrow accounts.
q) Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
r) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
s) Greater use of safe deposit facilities by individual, particularly the use of sealed packets which are deposited and soon withdrawn.

t) Substantial increase in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other clients company and trust accounts.
u) Large number of individuals making payments into the same account without an adequate explanation.
v) High velocity of funds that reflects the large volume of money flowing through an account.
w) An account opened in the name of name of a money changer that receives deposits.
x) An account operated in the name of an off-shore company with structured movement of funds

13.4 Trade Based Money Laundering

a) Over and under-invoicing of goods.
b) Multiple involving of goods and services
c) Over and under-invoicing of goods and services
d) Falsely described goods and services and “phantom” shipments where by the exporter does not ship any goods at all after payments and been made, particularly under confirmed letters of credit.
e) Transfer pricing
f) Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
g) Items shipped are inconsistent with the nature of the customer’s normal business and the transaction lacks an obvious economics rationale.
h) Customer requests payment of proceeds to an unrelated third party.
i) Significantly amended letters of credits without reasonable justification or changes to the beneficiary or location of payment.

13.5 Lending Activities

a) Customers who repay problem loans unexpectedly.

b) A customer who is reluctant or refuses to state the purpose of a loan or the source of repayment or repayment or provides a questionable purpose and/or source of repayment.
c) Loans secured by pledged assets held by third parties unrelated to the borrower.
d) Loans secured by deposits or other readily marketable assets, such as securities ,
e) Particularly when owned by apparently unrelated third parties.
f) Loans are made for, or are paid on behalf of a third party with no reasonable explanation.
g) Loans lack a legitimate business purpose, provide the bank with significant fees for assuming minimal risk, or tend to obscure the movement of funds (e.g. loans made to a borrower and immediately sold to an entity-related to borrower).

13.6 Terrorist Financing Red Flags

a) Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seems to corresponds to the stated occupation (e.g. student, unemployed, or self-employed).
b) Financial transaction by a nonprofit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.
c) A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
d) Large number of incoming or outgoing funds transfers takes place through a business account and there appears to be logical business or other economic purpose for the transfers, particularly when this activity involved designed high-risk locations.
e) The stated occupation of the customer is inconsistent with the type and level of account activity.
f) Funds transfer does not include information on the originator or the person on whose behalf the transaction is conducted the inclusion of which should ordinarily be expected.
g) Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

h) Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
i) Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

13.7 Other Unusual or Suspicious Activities

a) Employee exhibits a lavish lifestyles that cannot be justified by his/her salary
b) Employee fails to comply with approved operating guidelines particularly in private banking
c) Employee fails to comply with approved operating guidelines particularly in private banking
d) Employee is reluctant to make vacation.
e) Safe deposit boxes or safe custody accounts opened by individuals who do not reside work in the institution's service area despite the availability of such services at an institution closer to them.
f) Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high value assets awaiting conversion to currency, for placement in the banking system.
g) Customer uses a personal account for business purpose.
h) Official Embassy business is conducted through personal accounts
i) Embassy accounts are funded through substantial currency transactions.
j) Embassy accounts directly funds personal expenses of foreign nationals.

FCMB GROUP PLC

APPROVAL PAGE

PREPARED BY:

_____

Adetayo Olatunde – Head, Risk Management & Compliance DATE

REVIEWED BY:

_____

Babajide Odedele – Head, Internal Audit DATE

APPROVAL:

_____

Patrick Iyamabo – Chief Finance Officer DATE

_____

Peter Obaseki - Managing Director DATE